

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A quantitative competition method in which [[the]] a minimum value [[one]] V_{MIN} of all users² intended values V_{vi} selected from among M monotone increasing values V_w , where $w=1,2,\dots,M$, in [[the]] a range of predetermined lower-limit and upper-limit values V_1 and V_M , respectively, and only a user j having selected said minimum value V_{MIN} W_{MIN} as [[his]] an intended value V_{vi} are specified by a plurality of user apparatuses i , where $i=1,\dots,N$, said N being an integer equal to or larger than 2, first and second quantitative competition apparatuses, and a bulletin board apparatus that makes public information received from said plurality of user apparatuses and said first and second quantitative competition apparatuses, said method comprising:

Step (a) of generating two M -element sequences of information s_i and t_i , $i=1, 2, \dots, N$, wherein by each of said user apparatuses i [:]] responds in response to said intended value V_{vi} input by a user from one of said all users to generate two M -element sequences of information s_i and t_i , such that whose corresponding elements $s_{i,m}$ and $t_{i,m}$ of the sequences of information s_i and t_i equal each other at values in a [[the]] range from said lower-limit value V_1 inclusive or larger to said intended value V_{vi} exclusive or smaller and differ from each other at values in [[the]] a range from said intended value V_{vi} inclusive or larger to said upper-limit value V_M inclusive or smaller; and secretly sending sends information about said two M -element sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively, said M representing [[the]] a number of values selectable as said intended values in [[the]] a range from said lower-limit value V_1 inclusive or larger to said upper-limit value V_M inclusive or smaller;

Step (b) of extracting elements $s_{i,w}$ of said M -element sequences by wherein said first quantitative competition apparatus[:]] extracts, [[for]] corresponding to a given value V_w equal to or larger than said lower-limit value V_1 and equal to or smaller than said upper-limit value, these said elements $s_{i,w}$ of said M -element sequences of information s_i sent from said all user apparatuses which correspond to w ; and generates generating an element

concatenation $\text{Seq}_{s,w} = s_{1,w} || s_{2,w} || \dots || s_{N,w}$ in which said extracted elements $s_{i,w}$ are arranged in a predetermined order, said $||$ representing the concatenation of data;

Step (c) of extracting elements $t_{i,w}$ of said M-element sequences by wherein said second quantitative competition apparatus[[:]] extracts, [[for]] corresponding to said given value V_w , these said elements $t_{i,w}$ of said M-element sequences of information t_i sent from said all user apparatuses which correspond to said value w; and generates generating an element concatenation $\text{Seq}_{t,w} = t_{1,w} || t_{2,w} || \dots || t_{N,w}$ in which said extracted elements $t_{i,w}$ are arranged in a predetermined order;

Step (d) of comparing said element concatenations $\text{Seq}_{s,w}$ and $\text{Seq}_{t,w}$ without revealing their values by wherein said bulletin board apparatus,[[.]] compares said element concatenations $\text{Seq}_{s,w}$ and $\text{Seq}_{t,w}$ without revealing their values; decides deciding [[the]] presence or absence of a user having selected [[his]] an intended value equal to or smaller than said value V_w , depending on whether said concatenations $\text{Seq}_{s,w}$ and $\text{Seq}_{t,w}$ differ or equal; and determining determines [[the]] a minimum intended value V_{MIN} by changing said value w based on said deciding presence or absence decision and makes making [[the]] a value MIN public; and

Step (e) of sending element concatenations $\text{Seq}_{s,MIN}$ and $\text{Seq}_{t,MIN}$ from wherein said first and second quantitative competition apparatuses send element concatenations $\text{Seq}_{s,MIN}$ and $\text{Seq}_{t,MIN}$, respectively, to said bulletin board apparatus to make said element concatenations $\text{Seq}_{s,MIN}$ and $\text{Seq}_{t,MIN}$ them public, whereby allowing each user to identify user j who committed the minimum intended value V_{MIN} by finding j which satisfies $s_{j,MIN} \neq t_{j,MIN}$ of the corresponding elements in said element concatenations $\text{Seq}_{s,MIN}$ and $\text{Seq}_{t,MIN}$.

Claim 2 (Currently Amended): The method of claim 1, wherein:

said Step (a) includes[[:]] a step wherein said user apparatus of said each user i generates generating random numbers $R1_i$ and $R2_i$ and secretly sending send a pair of information $(R1_i, s_i)$ from said user apparatus of said each user i to said first quantitative competition apparatus and a pair of information $(R2_i, t_i)$ from said user apparatus of said each

user i to said second quantitative competition apparatus; and calculating a step wherein said user apparatus calculates hash values $H1_i = h(R1_i || s_i)$ and $H2_i = h(R2_i || t_i)$ of concatenations $R1_i || s_i$ and $R2_i || t_i$ of said pairs of information $(R1_i, s_i)$ and $(R2_i, t_i)$ by a hash function h by said user apparatus, and sends sending said hash values $H1_i$ and $H2_i$ to said bulletin board apparatus; and

 said Step (d) includes making public a step wherein said bulletin board apparatus makes public said hash values $H1_i$ and $H2_i$, where $i=1,2, \dots, N$, as commitments of said all users by said bulletin board apparatus.

3 (Currently Amended): The method of claim 2, wherein:

 said Step (b) includes calculating a step wherein said first quantitative competition apparatus: calculates a hash value $HS_w = h(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by said hash function h by said first quantitative competition apparatus; and sends sending said hash value HS_w to said bulletin board apparatus;

 said Step (c) includes calculating a step wherein said second quantitative competition apparatus: calculates a hash value $HT_w = h(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by said hash function h by said second quantitative competition apparatus; and sends sending said hash value HT_w to said bulletin board apparatus; and

 said Step (d) includes making a step wherein said bulletin board apparatus: makes public and comparing compares said hash values HS_w and HT_w received from said first and second quantitative competition apparatuses by said bulletin board apparatus; decides deciding [[the]] presence or absence of a user having selected [[his]] an intended value equal to or smaller than said value V_w , depending on whether said hash values HS_w and HT_w differ or equal; and determines determining said minimum intended value V_{MIN} by changing said value w based on deciding said presence or absence decision.

Claim 4 (Currently Amended): The method of claim 2, wherein:

said first and second quantitative competition apparatuses have stored therein a prime P made public previously by said bulletin board apparatus, said prime P being a prime such that $P-1$ has a large prime as its divisor, and said first and second quantitative competition apparatuses having selected a common integral value w ;

said Step (b) includes a step wherein said first quantitative competition apparatus: calculates calculating a hash value $HS_w = h'(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by a hash function h' that maps an arbitrary integer over a finite field uniquely and randomly by said first quantitative competition apparatus; generates generating a random number RA_w ; calculates calculating a hash value $HA_w = h(RA_w || HS_w)$ of a concatenation $RA_w || HS_w$ by said hash function h ; calculates calculating $HS_w^{RAw} \pmod{P}$; and sends sending a pair $(HA_w, HS_w^{RAw} \pmod{P})$ of said hash value HA_w and said value $HS_w^{RAw} \pmod{P}$ to said bulletin board apparatus;

said Step (c) includes a step wherein said second quantitative competition apparatus: calculates calculating a hash value $HT_w = h'(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by a hash function h' by said second quantitative competition apparatus; generates generating a random number RB_w ; calculates calculating a hash value $HB_w = h(RB_w || HT_w)$ of a concatenation $RB_w || HT_w$ by said hash function h ; calculates calculating $HT_w^{RBw} \pmod{P}$; and sends sending a pair $(HB_w, HT_w^{RBw} \pmod{P})$ of said hash value HB_w and said value $HT_w^{RBw} \pmod{P}$ to said bulletin board apparatus; and

said Step (d) includes: a step wherein said first quantitative competition apparatus reads reading said $HT_w^{RBw} \pmod{P}$ from said bulletin board apparatus by said first quantitative competition apparatus, and calculates calculating and sends sending $(HT_w^{RBw})^{RAw} \pmod{P}$ to said bulletin board apparatus; a step wherein said second quantitative competition apparatus reads reading said $HS_w^{RAw} \pmod{P}$ from said bulletin board apparatus by said second quantitative apparatus, and calculates calculating and sends sending $(HS_w^{RAw})^{RBw} \pmod{P}$ to said bulletin board apparatus; and a step wherein said bulletin board apparatus: makes making public and compares comparing said $(HS_w^{RAw})^{RBw} \pmod{P}$ and $(HT_w^{RBw})^{RAw} \pmod{P}$ received from said first and second quantitative competition

apparatuses; decides deciding [[the]] presence or absence of a user having selected [[his]] an intended value equal to or smaller than said value V_w , depending on whether said $(HS_w^{RAw})^{RBw} \pmod{P}$ and $(HT_w^{RBw})^{RAw} \pmod{P}$ differ or equal; and determines determining said minimum intended value V_{MIN} by changing said value w based on said deciding presence or absence decision.

Claim 5 (Currently Amended): The method of claim 3 or 4, wherein: letting w_{min} and w_{max} represent variables, said first and second quantitative competition apparatuses have said value w in common as [[the]] a maximum integer equal to or smaller than $(w_{min}+w_{max})/2=(1+M)/2$ where $w_{min}=1$ and $w_{max}=M$; and

 said Step (d) includes a step wherein: substituting w is substituted for with said variable w_{max} or substituting $w+1$ is substituted for with said variable w_{min} , depending on [[the]] presence or absence of a user having selected [[his]] an intended value equal to or smaller than said value V_w ; said Steps (b) and (c) are repeated until $w_{max}=w_{min}=MIN$, thereby obtaining to obtain said minimum intended value V_{MIN} corresponding to said value MIN ; and upon each repetition of said Steps (b) and (c), said bulletin board apparatus makes public the results of calculation.

Claim 6 (Original): The method of claim 4, wherein each element of said M -element sequences of information s_i and t_i is a one-bit element.

Claim 7 (Currently Amended): The method of claim 4 or 6, wherein said step (e) includes sending further comprising a step wherein said first and second quantitative competition apparatus send said bulletin board apparatus random numbers RA_{MIN} and RB_{MIN} from said first and second quantitative competition apparatus to said bulletin board apparatus making said random numbers RA_{MIN} and RB_{MIN} and make them public.

Claim 8 (Currently Amended): The method of any one of claims 1 to 4, wherein: L quantitative competition apparatuses are provided, said L being equal to or larger than 3; said Step (a) includes generating L sequences of information s_{ik} where $k=1,2, \dots, L$, by said each user apparatus, a step wherein when supplied with said value V_{vi} , said each user apparatus generates L sequences of information s_{ik} , where $k=1,2, \dots, L$, said L sequences of information s_{ik} being such that they are equal in all pieces of information corresponding to values equal to or greater than V_1 and equal to or smaller than V_{vi} but different in all pieces of information corresponding to values equal to or larger than V_{vi} and equal to or smaller than V_M and such that said value V_{vi} can be detected when at least two sequences s_{ia} and s_{ib} of said L sequences of information s_{ik} are known, where $a \neq b$; and secretly sending said each user apparatus sends said L sequences of information s_{ik} to a k-th quantitative competition apparatus; and

wherein two of said L quantitative competition apparatuses conduct quantitative competition, and when one of said two quantitative competition apparatuses goes down, another normal one of the a remaining operable quantitative competition apparatuses is used to continue said quantitative competition.

Claim 9 (Currently Amended): The method of claim 1, wherein said Step (a) includes a step wherein: said each user apparatus secretly sending sends seed values s'_i and t'_i , by said each user apparatus, as information corresponding to said two sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively; wherein letting vi represent the element number corresponding to said intended value V_{vi} , said seed values s'_i and t'_i are determined by a one-way function F so that $F^d(s'_i) = F^d(t'_i)$, where $d=0,1, \dots, M-vi$, and $F^e(s'_i) = F^e(t'_i)$, where $e=M-vi+1, \dots, M-1$; and said two sequences of information s_i and t_i are given by the following equations

$$s_i = \{s_{i,1} = F^{M-1}(s'_i), s_{i,2} = F^{M-2}(s'_i), \dots, s_{i,vi-1} = F^{M-vi+1}(s'_i), s_{i,vi} = F^{M-vi}(s'_i), \dots,$$

$$s_{i,M-1} = F(s'_i), s_{i,M} = s'_i\} \text{ and}$$

$$t_i = \{t_{i,1} = F^{M-1}(t'_i), t_{i,2} = F^{M-2}(t'_i), \dots, t_{i,vi-1} = F^{M-vi+1}(t'_i), t_{i,vi} = F^{M-vi}(t'_i), \dots,$$

$t_{i,M-1}=F(t'_{i,1})$, $t_{i,M}=s'_{i,1}$.

Claim 10 (Currently Amended): The method of claim 1, wherein said Step (a) includes:

~~a step wherein said each user apparatus generates generating~~ initial random numbers $R_{1,i}$, $R_{2,i}$, ca_i , cb_i , $s_{i,M+1}$ and $t_{i,M+1}$ by said each user apparatus; and
~~a step wherein said each user apparatus: sets setting~~ an initial value of m at M , and performing, performs, with respect to the element number vi corresponding to said intended value V_{vi} , the following calculations by said each user apparatus

$$s_{i,m}=h(s_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i)) \text{ and}$$

$$t_{i,m}=h(t_{i,m+1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

sequentially for $m=M, M-1, \dots, vi$ to provide subsequences $s_{i,m} \neq t_{i,m}$; calculates calculating a sequence element for $m=vi-1$

$$s_{i,m}=t_{i,m}=h(s_{i,m-1}||t_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

and a sequence element for $m=vi-2, vi-3, \dots, 0$

$$s_{i,m}=t_{i,m}=h(s_{i,m-1}||h^{M+1-m}(ca_i)||h^{M+1-m}(cb_i))$$

to provide subsequences $s_{i,m}=t_{i,m}$; and obtains obtaining sequences of said elements $s_{i,m}$ and $t_{i,m}$ as said sequences of information s_i and t_i , and a value $s_{i,0}$ for $m=0$; and

wherein said Step (a) further includes ~~a step wherein said each user apparatus encrypts encrypting~~ $R_{1,i}$ and $s_i=\{s_{i,1}, s_{i,2}, \dots, s_{i,M}\}$ by an encryption function E_A by said each user apparatus, sends sending a [[the]] resulting $E_A(s_i||R_{1,i})$ to said first quantitative competition apparatus, ~~encrypts encrypting~~ $R_{2,i}$ and $t_i=\{t_{i,1}, t_{i,2}, \dots, t_{i,M}\}$ by an encryption function E_B , and sends sending a [[the]] resulting $E_B(t_i||R_{2,i})$ to said second quantitative competition apparatus; and ~~a step wherein said each user apparatus sends sending~~ $H_{1,i}=h(s_i||R_{1,i})$, $H_{2,i}=h(t_i||R_{2,i})$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ from said each user apparatus to said bulletin board to make them said $H_{1,i}=h(s_i||R_{1,i})$, $H_{2,i}=h(t_i||R_{2,i})$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ public.

Claim 11 (Currently Amended): A quantitative competition method in which a [[the]] maximum value [[one]] V_{MAX} of all users' intended values V_{vi} selected from among M monotone increasing values V_w , where $w=1,2,\dots, M$, in [[the]] a range of predetermined lower-limit and upper-limit values V_1 and V_M , respectively, and only a user j having selected said maximum value V_{MAX} W_{MAX} as [[his]] an intended value V_{vi} are specified by a plurality of user apparatuses i , where $i=1,\dots, N$, said N being an integer equal to or larger than 2, first and second quantitative competition apparatuses, and a bulletin board apparatus that makes public information received from said plurality of user apparatuses and said first and second quantitative competition apparatuses, said method comprising:

Step (a) of generating two M-element sequences of information s_i and t_i , $i=1, 2, \dots, N$, wherein by each of said user apparatuses i [:]] responds in response to said intended value V_{vi} input by a user from one of said all users to generate two M-element sequences of information s_i and t_i , such that whose corresponding elements $s_{i,m}$ and $t_{i,m}$ of the sequences of information s_i and t_i equal each other at values in a [[the]] range from said lower-limit value V_1 inclusive or larger to said intended value V_{vi} inclusive or smaller and differ from each other at values in [[the]] a range from said intended value V_{vi} exclusive or larger to said upper-limit value V_M inclusive or smaller; and secretly sending sends information about said two M-element sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively, said M representing [[the]] a number of values selectable as said intended values in [[the]] a range from said lower-limit value V_1 inclusive or larger to said upper-limit value V_M inclusive or smaller;

Step (b) of extracting elements $s_{i,w}$ of said M-element sequences by wherein said first quantitative competition apparatus[:]] extracts, [[for]] corresponding to a given value V_w equal to or larger than said lower-limit value V_1 and equal to or smaller than said upper-limit value, these said elements $s_{i,w}$ of said M-element sequences of information s_i sent from said all user apparatuses which correspond to w ; and generates generating an element concatenation $Seq_{s,w}=s_{1,w}||s_{2,w}||\dots||s_{N,w}$ in which said extracted elements $s_{i,w}$ are arranged in a predetermined order, said || representing the concatenation of data;

Step (c) of extracting elements $t_{i,w}$ of said M-element sequences by wherein said second quantitative competition apparatus $[[::]]$ extracts, [[for]] corresponding to said given value V_w , these said elements $t_{i,w}$ of said M-element sequences of information t_i sent from said all user apparatuses which correspond to said value w ; and generates generating an element concatenation $Seq_{t,w}=t_{1,w}||t_{2,w}||\dots||t_{N,w}$ in which said extracted elements $t_{i,w}$ are arranged in a predetermined order;

Step (d) of comparing said element concatenations $Seq_{s,w}$ and $Seq_{t,w}$ without revealing their values by wherein said bulletin board apparatus $[[::]]$ compares said element concatenations $Seq_{s,w}$ and $Seq_{t,w}$ without revealing their values; decides deciding [[the]] presence or absence of a user having selected [[his]] an intended value equal to or larger than said value V_w , depending on whether said concatenations $Seq_{s,w}$ and $Seq_{t,w}$ differ or equal; and determining a determines the maximum intended value V_{MAX} by changing said value w based on said deciding presence or absence decision and makes a [[the]] value MAX public; and

Step (e) of sending element concatenations $Seq_{s,MIN}$ and $Seq_{t,MIN}$ from wherein said first and second quantitative competition apparatuses send element concatenations $Seq_{s,MAX}$ and $Seq_{t,MAX}$, respectively, to said bulletin board apparatus to make said element concatenations $Seq_{s,MIN}$ and $Seq_{t,MIN}$ them public, whereby allowing each user to identify user j who committed the maximum intended value V_{MAX} by finding j which satisfies $s_{j,MAX} \neq t_{j,MAX}$ of the corresponding elements in said element concatenations $Seq_{s,MAX}$ and $Seq_{t,MAX}$.

Claim 12 (Currently Amended): The method of claim 11, wherein:

~~said Step (a) includes[[::]] a step wherein said user apparatus of said each user i generates generating random numbers $R1_i$ and $R2_i$ and secretly sending send a pair of information $(R1_i, s_i)$ from said user apparatus of said each user i to said first quantitative competition apparatus, and a pair of information $(R2_i, t_i)$ from said user apparatus of said each user i to said second quantitative competition apparatus; and calculating a step wherein said user apparatus calculates hash values $H1_i=h(R1_i||s_i)$ and $H2_i=h(R2_i||t_i)$ of concatenations~~

R1_i||s_i and R2_i||t_i of said pairs of information (R1_i, s_i) and (R2_i, t_i) by a hash function h by said user apparatus, and sends sending said hash values H1_i and H2_i to said bulletin board apparatus; and

 said Step (d) includes making public a step wherein said bulletin board apparatus makes public said hash values H1_i and H2_i, where i=1,2, ..., N, as commitments of said all users by said bulletin board apparatus.

Claim 13 (Currently Amended): The method of claim 12, wherein:

 said Step (b) includes calculating a step wherein said first quantitative competition apparatus calculates a hash value HS_w=h(Seq_{s,w}) of said element concatenation Seq_{s,w} by said hash function h by said first quantitative competition apparatus; and sends sending said hash value HS_w to said bulletin board apparatus;

 said Step (c) includes calculating a step wherein said second quantitative competition apparatus calculates a hash value HT_w=h(Seq_{t,w}) of said element concatenation Seq_{t,w} by said hash function h by said second quantitative competition apparatus; and sends sending said hash value HT_w to said bulletin board apparatus; and

 said Step (d) includes making a step wherein said bulletin board apparatus makes public and comparing compares said hash values HS_w and HT_w received from said first and second quantitative competition apparatuses by said bulletin board apparatus; decides deciding [[the]] presence or absence of a user having selected [[his]] an intended value equal to or larger than said value V_w, depending on whether said hash values HS_w and HT_w differ or equal; and determines determining said maximum intended value V_{MAX} by changing said value w based on said deciding presence or absence decision.

Claim 14 (Currently Amended): The method of claim 12, wherein:

 said first and second quantitative competition apparatuses have stored therein a prime P made public previously by said bulletin board apparatus, said prime P being a prime such

that P-1 has a large prime as its divisor, and said first and second quantitative competition apparatuses having selected a common integral value w;

 said Step (b) includes a step wherein said first quantitative competition apparatus: calculates calculating a hash value $HS_w = h'(Seq_{s,w})$ of said element concatenation $Seq_{s,w}$ by a hash function h' that maps an arbitrary integer over a finite field uniquely and randomly by said first quantitative competition apparatus; generates generating a random number RA_w ; calculates calculating a hash value $HA_w = h(RA_w || HS_w)$ of a concatenation $RA_w || HS_w$ by said hash function h ; calculates calculating $HS_w^{RAw} \pmod{P}$; and sends sending a pair $(HA_w, HS_w^{RAw} \pmod{P})$ of said hash value HA_w and said value $HS_w^{RAw} \pmod{P}$ to said bulletin board apparatus;

 said Step (c) includes a step wherein said second quantitative competition apparatus: calculates calculating a hash value $HT_w = h'(Seq_{t,w})$ of said element concatenation $Seq_{t,w}$ by a hash function h' by said second quantitative competition apparatus; generates generating a random number RB_w ; calculates calculating a hash value $HB_w = h(RB_w || HT_w)$ of a concatenation $RB_w || HT_w$ by said hash function h ; calculates calculating $HT_w^{RBw} \pmod{P}$; and sends sending a pair $(HB_w, HT_w^{RBw} \pmod{P})$ of said hash value HB_w and said value $HT_w^{RBw} \pmod{P}$ to said bulletin board apparatus; and

 said Step (d) includes: a step wherein said first quantitative competition apparatus reads reading said $HT_w^{RBw} \pmod{P}$ from said bulletin board apparatus by said first quantitative competition apparatus, and calculates calculating and sends sending $(HT_w^{RBw})^{RAw} \pmod{P}$ to said bulletin board apparatus; a step wherein said second quantitative competition apparatus reads reading said $HS_w^{RAw} \pmod{P}$ from said bulletin board apparatus by said second quantitative competition apparatus, and calculates calculating and sends sending $(HS_w^{RAw})^{RBw} \pmod{P}$ to said bulletin board apparatus; and a step wherein said bulletin board apparatus: makes making public and compares comparing said $(HS_w^{RAw})^{RBw} \pmod{P}$ and $(HT_w^{RBw})^{RAw} \pmod{P}$ received from said first and second quantitative competition apparatuses; decides the deciding presence or absence of a user having selected [[his]] an intended value equal to or larger than said value V_w , depending on

whether said $(HS_w^{RAW})^{RBw} \pmod{P}$ and $(HT_w^{RBw})^{RAW} \pmod{P}$ differ or equal; and determining determines said maximum intended value V_{MAX} by changing said value w based on said deciding presence or absence decision.

Claim 15 (Currently Amended): The method of claim 13 or 14, wherein: letting w_{min} and w_{max} represent variables of integers 1 to M, said first and second quantitative competition apparatuses have said value w in common as [[the]] a maximum integer equal to or smaller than $(w_{min}+w_{max})/2=(1+M)/2$ where $w_{min}=1$ and $w_{max}=M$; and

 said Step (d) includes substituting a step wherein: w is substituted for with said variable w_{max} or substituting w+1 is substituted for with said variable w_{min} , depending on [[the]] presence or absence of a user having selected [[his]] an intended value equal to or larger than said value V_w ; said Steps (b) and (c) are repeated until $w_{max}=w_{min}=MAX$, thereby obtaining to obtain said minimum intended value V_{MAX} corresponding to said value MAX; and upon each repetition of said Steps (b) and (c), said bulletin board apparatus makes public the results of calculation.

Claim 16 (Original): The method of claim 14, wherein each element of said M-element sequences of information s_i and t_i is a one-bit element.

Claim 17 (Currently Amended): The method of claim 14 or 16, said step (e) includes sending further comprising a step wherein said first and second quantitative competition apparatus send said bulletin board apparatus random numbers RA_{MIN} and RB_{MIN} from said first and second quantitative competition apparatus to said bulletin board apparatus, respectively, making public said random numbers RA_{MIN} and RB_{MIN} to make them public.

Claim 18 (Currently Amended): The method of any one of claims 11 to 14, wherein: L quantitative competition apparatuses are provided, said L being equal to or larger than 3;

said Step (a) includes generating L sequences of information s_{ik} , where $k=1,2, \dots, L$, by said each user apparatus, a step wherein when supplied with said value V_{vi} , said each user apparatus generates L sequences of information s_{ik} , where $k=1,2, \dots, L$, said L sequences of information s_{ik} being such that they are equal in all pieces of information corresponding to values equal to or greater than V_1 and smaller than V_{vi} but different in all pieces of information corresponding to values equal to or larger than V_{vi} and equal to or smaller than V_M and such that said value V_{vi} can be detected when at least two sequences s_{ia} and s_{ib} of said L sequences of information s_{ik} are known, where $a \neq b$; and sending said each user apparatus sends said L sequences of information s_{ik} to a k-th quantitative competition apparatus; and

wherein two of said L quantitative competition apparatuses conduct quantitative competition, and when one of said two quantitative competition apparatuses goes down, another normal one of the a remaining operable quantitative competition apparatuses is used to continue said quantitative competition.

Claim 19 (Currently Amended): The method of claim 11, wherein said Step (a) includes a step wherein: said each user apparatus secretly sends sending seed values s'_i and t'_i , by said each user apparatus, as information corresponding to said two sequences of information s_i and t_i to said first and second quantitative competition apparatuses, respectively; wherein letting vi represent the element number corresponding to said intended value V_{vi} , said seed values s'_i and t'_i are determined by a one-way function F so that $F^d(s'_i) = F^d(t'_i)$, where $d=0,1, \dots, M-vi$, and $F^e(s'_i) = F^e(t'_i)$, where $e= M-vi+1, \dots, M-1$; and said two sequences of information s_i and t_i are given by the following equations

$$s_i = \{s_{i,1}=F^{M-1}(s'_i), s_{i,2}=F^{M-2}(s'_i), \dots, s_{i,vi-1}=F^{M-vi+1}(s'_i), s_{i,vi}=F^{M-vi}(s'_i), \dots,$$

$$s_{i,M-1}=F(s'_i), s_{i,M}=s'_i\} \text{ and}$$

$$t_i = \{t_{i,1}=F^{M-1}(t'_i), t_{i,2}=F^{M-2}(t'_i), \dots, t_{i,vi-1}=F^{M-vi+1}(t'_i), t_{i,vi}=F^{M-vi}(t'_i), \dots,$$

$$t_{i,M-1}=F(t'_i), t_{i,M}=s'_i\}.$$

Claim 20 (Currently Amended): The method of claim 11, wherein said Step (a) includes:

~~a step wherein said each user apparatus generates generating~~ initial random numbers R_{1i} , R_{2i} , ca_i , cb_i , $s_{i,M+1}$ and $t_{i,M+1}$ by said each user apparatus; and
~~a step wherein said each user apparatus: sets setting~~ an initial value of m at M , and performs performing, with respect to the element number vi corresponding to said intended value V_{vi} , the following calculations by said each user apparatus

$$s_{i,m} = h(s_{i,m+1} || h^{M+1-m}(ca_i) || h^{M+1-m}(cb_i)) \text{ and}$$

$$t_{i,m} = h(t_{i,m+1} || h^{M+1-m}(ca_i) || h^{M+1-m}(cb_i))$$

sequentially for $m=M, M-1, \dots, vi$ to provide subsequences $s_{i,m} \neq t_{i,m}$; calculates calculating a sequence element for $m=vi-1$

$$s_{i,m} = t_{i,m} = h(s_{i,m-1} || t_{i,m-1} || h^{M+1-m}(ca_i) || h^{M+1-m}(cb_i))$$

and a sequence element for $m=vi-2, vi-3, \dots, 0$

$$s_{i,m} = t_{i,m} = h(s_{i,m-1} || h^{M+1-m}(ca_i) || h^{M+1-m}(cb_i))$$

to provide subsequences $s_{i,m} = t_{i,m}$; and obtains obtaining sequences of said elements $s_{i,m}$ and $t_{i,m}$ as said sequences of information s_i and t_i , and a value $s_{i,0}$ for $m=0$; and

wherein said Step (a) further includes: ~~a step wherein said each user apparatus encrypts encrypting~~ R_{1i} and $s_i = \{s_{i,1}, s_{i,2}, \dots, s_{i,M}\}$ by an encryption function E_A by said each user apparatus, sends sending a [[the]] resulting $E_A(s_i || R_{1i})$ to said first quantitative competition apparatus, ~~encrypts encrypting~~ R_{2i} and $t_i = \{t_{i,1}, t_{i,2}, \dots, t_{i,M}\}$ by an encryption function E_B , and sends sending a [[the]] resulting $E_B(t_i || R_{2i})$ to said second quantitative competition apparatus; and ~~a step wherein said each user apparatus sends sending~~ $H_{1i} = h(s_i || R_{1i})$, $H_{2i} = h(t_i || R_{2i})$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ from said each user apparatus to said bulletin board to make said $H_{1i} = h(s_i || R_{1i})$, $H_{2i} = h(t_i || R_{2i})$, $s_{i,0}$, $h^{M+1}(ca_i)$ and $h^{M+1}(cb_i)$ them public.

Claim 21 (Currently Amended): The method of claim 1 or 11, wherein said Step (a) includes ~~a step wherein said each user apparatus: generates generating~~ a random number r_i by

said each user apparatus; determines determining two pieces of random information a_i and b_i , where $r_i = a_i * b_i$, said symbol * being a predetermined common operator; sends sending said pieces of random information a_i and b_i to said first and second quantitative competition apparatuses, respectively; hashes hashing said pieces of random information a_i and b_i by a hash function h ; and sending sends hash values $h(a_i)$, $h(b_i)$ and $h(V_{vi}||r_i)$ to said bulletin board apparatus; and said Step (e) includes ~~a step wherein said first and second quantitative apparatuses send~~ sending said pieces of random information a_j and b_j ~~from said first and second quantitative apparatuses~~ to said bulletin board apparatus making said pieces of random information a_j and b_j to make them public, and ~~said each user apparatus verifies~~ verifying, by said each user apparatus, [[said]] made-public hash values $h(a_j)$ and $h(b_j)$ by using [[said]] made-public random information a_j and b_j and further verifying verifies whether $h(V_{vj}||r_i) = h(V_{vj}||a_j * b_j)$.

Claim 22 (Currently Amended): A method by which said each user apparatus in said quantitative competition method of claim 1 registers [[his]] an intended value V_{vi} selected from among M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2, said method comprising the steps of:

(a) responding to [[the]] input of said intended value V_{vi} to generate two M -element sequences of information s_i and t_i , wherein whose corresponding elements of said two M -element sequences of information s_i and t_i equal each other at values in a [[the]] range from said value V_1 inclusive V_i or larger to said value V_{vi} exclusive or smaller and differ from each other at values in a [[the]] range from said value V_{vi} inclusive or larger to said value V_M inclusive or smaller;

(b) responding to the input of said two M -element sequences of information s_i and t_i to calculate one-way functions [[for]] of said sequences of information s_i and t_i and send sending calculation results $H1_i$ and $H2_i$ to a bulletin board apparatus; and

(c) sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to said bulletin board apparatus.

Claim 23 (Currently Amended): A method by which said each user apparatus in said quantitative competition method of claim 11 registers [[his]] an intended value V_{vi} selected from among M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2, said method comprising the steps of:

(a) responding to [[the]] input of said intended value V_{vi} to generate two M -element sequences of information s_i and t_i , wherein whose corresponding elements of said two M -element sequences of information s_i and t_i differ from each other at values in [[the]] a range from said value V_1 inclusive or larger to said value V_{vi} inclusive or smaller and equal each other at values in [[the]] a range from a value V_{vi+1} inclusive or larger to said value V_M inclusive or smaller;

(b) responding to the input of said two M -element sequences of information s_i and t_i to calculate one-way functions [[for]] of said sequences of information s_i and t_i and send sending calculation results $H1_i$ and $H2_i$ to a bulletin board apparatus; and

(c) sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to said bulletin board apparatus.

Claim 24 (Currently Amended): A user apparatus for use in said quantitative competition method of claim 1, comprising:

a storage part configured to store having stored therein M integral values defined by upper and lower limits V_M and V_1 for comparison;

an input part configured to input means for inputting an intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M ;

a sequence-of-information generating part supplied with said values V_{vi} , V_1 and V_M , ~~for generating and outputting configured to generate and output~~ two M-element sequences of information s_i and t_i , ~~wherein whose~~ corresponding elements ~~of said two M-element sequences of information~~ s_i and t_i equal ~~each other at values in~~ $[[the]]$ a range from said lower-limit value V_1 ~~inclusive or larger~~ to said intended value V_{vi} ~~exclusive or smaller~~ and differ ~~from each other at values in~~ $[[the]]$ a range from said intended value V_{vi} ~~inclusive or larger~~ to said upper-limit value V_M ~~inclusive or smaller~~, or two M-element sequences of information s_i and t_i , ~~wherein whose~~ corresponding elements ~~of said two M-element sequences of information~~ s_i and t_i differ ~~from each other at values in~~ $[[the]]$ a range from said lower-limit value V_1 ~~inclusive or larger~~ to said intended value V_{vi} ~~inclusive or smaller~~ and equal ~~each other at values in~~ $[[the]]$ a range from a value V_{vi+1} ~~inclusive or larger~~ to said upper-limit value V_M ~~inclusive or smaller~~, said M being $[[the]]$ a number of values selectable as said intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M ;

a one-way function calculating part, supplied with said sequences of information s_i and t_i , ~~for calculating configured to calculate~~ one-way functions $[[for]]$ ~~of~~ said sequences of information s_i and t_i and ~~output for outputting~~ calculation results $H1_i$ and $H2_i$; and

a transmitting part ~~configured to send for sending~~ said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to a bulletin board apparatus.

Claim 25 (Currently Amended): A user apparatus for use in said quantitative competition method of claim 11, comprising:

a storage part ~~configured to store having stored therein~~ M integral values defined by upper and lower limits V_M and V_1 for comparison, said M being an integer equal to or larger than 2;

~~an input part configured to input means for inputting~~ an intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M ;

a sequence-of-information generating part, supplied with said values V_{vi} , V_1 and V_M , ~~for generating and outputting configured to generate and output~~ two M-element sequences of information s_i and t_i , ~~wherein whose~~ corresponding elements ~~of said two M-element sequences of information~~ s_i and t_i differ ~~from each other at values in a~~ the range from said lower-limit value V_1 ~~inclusive or larger~~ to said intended value V_{vi} ~~inclusive or smaller~~ and equal ~~each other at values in [[the]]~~ a range from a value V_{vi+1} ~~inclusive or larger~~ to said upper-limit value V_M ~~inclusive or smaller~~;

a one-way function calculating part, supplied with said sequences of information s_i and t_i , ~~configured to calculate for calculating~~ one-way functions [[for]] ~~of~~ said sequences of information s_i and t_i and ~~output for outputting~~ calculation results H_{1i} and H_{2i} ; and

a transmitting part ~~configured to send for sending~~ said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said H_{1i} and H_{2i} to a bulletin board apparatus.

Claim 26 (Currently Amended): A quantitative competition apparatus for use in a quantitative competition method of claim 1 or 11, comprising:

a receiving part ~~configured to receive for receiving~~ from each user apparatus a sequence of information consisting of elements of [[the]] a same number M as that of values selectable as an intended value V_{vi} in [[the]] a range [[of]] between lower-limit value V_1 and upper-limit value V_1 and V_M , inclusively, and ~~for receiving~~ an integral value w from a bulletin board apparatus;

a storage part ~~configured to store for storing~~ said sequence of information received from said each user apparatus;

a one-way function calculating part, supplied with w -th elements of said sequences of information received from users, ~~for calculating and outputting configured to calculate and output~~ one-way functions [[for]] ~~of~~ concatenations of said w -th elements; and

a transmitting part ~~configured to send for sending~~ said calculated one-way functions to said bulletin board apparatus.

Claim 27 (Currently Amended): A competition method by a quantitative competition apparatus for use in said quantitative competition method of claim 1 or 11, said method comprising the steps of:

- (a) receiving, from each user apparatus i , where $i=1,2,\dots,N$, an M -element sequence of information $s_i=\{s_{i,1} s_{i,2}, \dots, s_{i,M}\}$ as information representing an intended value V_{vi} selected from among M values in [[the]] a range [[of]] between lower-limit value V_1 and upper-limit value V_1 and V_M , inclusively;
- (b) receiving an integral value w from a bulletin board apparatus;
- (c) inputting a w -th element $s_{i,w}$ of said sequence of information s_i received from said each user apparatus and calculating a one-way function [[for]] of a concatenation of such input w -th elements $s_{i,w}$; and
- (d) sending said calculated one-way function to said bulletin board.

Claim 28 (Currently Amended): A quantitative competition apparatus for use in said quantitative competition method of claim 1 or 11, said apparatus comprising:

a receiving part configured to receive ~~for receiving~~ from each user apparatus a sequence of information consisting of elements of [[the]] a same number M as that of values selectable as an intended value V_{vi} in [[the]] a range [[of]] between lower-limit value V_1 and upper-limit value V_1 and V_M , inclusively, and ~~for receiving~~ an integral value w from a bulletin board apparatus;

a storage part configured to store ~~for storing~~ said sequence of information received from said each user apparatus;

a one-way function calculating part, supplied with w -th elements of said sequences of information received from users, ~~for calculating and outputting~~ configured to calculate and output one-way functions [[for]] of concatenations of said w -th elements; and

a transmitting part configured to send ~~for sending~~ said calculated one-way functions to said bulletin board apparatus.

Claim 29 (Currently Amended): A computer program for executing the procedure to be followed by a user apparatus in a quantitative competition method of claim 1 or 11, said program comprising the steps of:

responding to an intended value V_{vi} selected from among integral values defined by upper-limit value V_1 and lower-limit value values V_1 and V_M , inclusively, for comparison to generate two M-element sequences of information s_i and t_i , wherein whose corresponding elements of said two M-element sequences of information s_i and t_i equal each other at values in [[the]] a range from said lower-limit value V_1 inclusive or larger to said intended value V_{vi} exclusive or smaller and differ from each other at values in [[the]] a range from said intended value V_{vi} inclusive or larger to said upper-limit value V_M inclusive or smaller, or two M-element sequences of information s_i and t_i , wherein whose corresponding elements of said two M-element sequences of information s_i and t_i differ from each other at values in [[the]] a range from said lower-limit value V_1 inclusive or larger to said intended value V_{vi} inclusive or smaller and equal each other at values in [[the]] a range from a value V_{vi+1} inclusive or larger to said upper-limit value V_M inclusive or smaller, said M being the number of values selectable as said intended value V_{vi} equal to or larger than said value V_1 and equal to or smaller than said value V_M ;

calculating one-way functions [[for]] of said sequences of information s_i and t_i and [[for]] outputting calculation results $H1_i$ and $H2_i$; and

sending said sequence of information s_i to a first quantitative competition apparatus, said sequence of information t_i to a second quantitative competition apparatus, and said $H1_i$ and $H2_i$ to a bulletin board apparatus.

Claim 30 (Original): A recording medium on which there is recorded said computer program of claim 29.